

REMARKS

This Application has been carefully reviewed in light of the Final Official Action dated December 16, 2002. In order to advance prosecution of the present Application, Claims 1, 12, and 23 have been amended. Applicant respectfully requests reconsideration and favorable action for this Application.

Claims 12-22 stand rejected under 35 U.S.C. §102(e) as being anticipated by Burnett, et al. Independent Claim 12 recites in general a connections property table in a client network used to generate keys to gain access to a server network. By contrast, the Burnett, et al. patent has an authenticator routine associated with a server system that determine whether a client request can be satisfied. Thus, all authentication for a request is performed in the server station as opposed to the client station and there is no connections property table in the client station of the Burnett, et al. patent as provided by the claimed invention. Moreover, the Burnett, et al. patent specifically states that its client station need not know anything about the source of the object being requested and thus teaches away from the claimed invention. See col. 8, lines 1-13 of the Burnett, et al. patent. Further, the Examiner readily admits that the Burnett, et al. patent fails to disclose a connection properties table located at a client network. Support for the above recitation can be found at page 14, lines 10-12, of Applicant's specification. Therefore, Applicant respectfully submits that Claims 12-22 are not anticipated by the Burnett, et al. patent.

Claims 1-11 and 23-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Burnett, et al. in view of Quinlan. Applicant respectfully traverses this rejection.

There is no suggestion or motivation in the Burnett, et al. and Quinlan patents to combine them as proposed by the

Examiner. The Burnett, et al. patent is directed to a method for providing authenticated access to files at a server system in response to requests from a client system. The Quinlan patent is directed to the use of session pools to initiate new session connections or establish previously existing session connections without having an authentication requirement. Thus, none of the cited patents are related to any common subject matter. Moreover, the Examiner has not cited any language within either the Burnett, et al. or Quinlan patents that would suggest any capability for them to be combined despite their unrelated subject matter. The portions of the Quinlan patent cited by the Examiner to support combination with the Burnett, et al. patent merely addresses where state information pertaining to a connection session is located in a client network but does not address any aspect of authentication as provided in the Burnett, et al. patent. The Examiner merely uses isolated portions of the cited references to provide a conclusory subjective reasoning in support of their combination without looking at what the references teach as a whole as is required by M.P.E.P. §2141.02. Absent any support from within the patents as a whole to combine them as has been proposed, the Examiner is applying an improper hindsight reconstruction of the claimed invention from the bits and pieces of isolated citations in the references. Further, the Burnett, et al. patent provides for authentication control in a server system while the Quinlan patent addresses removing responsibilities from the server system by placing session connection maintenance in its client system. Thus, the server system burden removal concept of the Quinlan patent is in contrast with the server system authentication control concept of the Burnett, et al. patent. Also, each reference has been placed into separate and distinct classifications in the U.S. Patent and Trademark

Office that have no obvious relationship to each other. Therefore, Applicant respectfully submits that the Burnett, et al. and Quinlan patents have been improperly combined by the Examiner.

Moreover, even if the references were capable of being combined, their resulting structure does not meet the terms of the claims. Independent Claims 1 and 23 recite in general the formation of a boundary traversal key from a connections property table at a client network having information to traverse a boundary controlling access to a server network and forwarding the boundary traversal key to the boundary controlling access to the server network. By contrast, the Burnett, et al. patent performs its authentication process at its server system and has no connections property table at its client system while the Quinlan patent merely maintains session connections with no authentication capability or boundaries to traverse. Thus, the Examiner's proposed combination of the server system controlled authentication process of the Burnett, et al. patent with the session connection maintenance technique of the Quinlan patent, which makes no mention of authentication or boundary traversal, would still lack the ability to provide a connections property table at a client network having information to generate a boundary traversal key in order to traverse a boundary controlling access to a server network as required by the claimed invention. Therefore, Applicant respectfully submits that Claims 1-11 and 23-27 are patentably distinct from the proposed Burnett, et al. - Quinlan combination.

Applicant respectfully submits that the Examiner has improperly made this Office Action final. Pursuant to M.P.E.P. §706.07(a), a second action on the merits will not be made final if it includes a rejection on newly cited art of any claim not amended in spite of the fact that other claims

may have been amended to require newly cited art. In this Application, Claim 23 was rejected in the first Office Action under 35 U.S.C. §102(e) as being anticipated by Burnett, et al. Now, the Examiner rejects Claim 23 in this 'final' Office Action as being unpatentable over Burnett, et al. in view of Quinlan. However, Applicant made no amendment to Claim 23 that necessitated the Examiner's new ground of rejection nor did Applicant submit the newly cited Quinlan patent in an information disclosure statement. Thus, this second action on the merits can not be made final as the new ground of rejection presented by the Examiner with respect to Claim 23 was neither necessitated by any amendment of the Applicant nor based on an information disclosure statement filed by the Applicant. Therefore, Applicant respectfully requests the improper finality of the present Office Action be withdrawn.

Applicant has now made an earnest attempt to place the Application in condition for allowance. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests reconsideration and full allowance of Claims 1-27.

The present Response to Examiner's Final Action is necessary to address new grounds of rejection and newly cited art not previously presented by the Examiner and to raise the improper finality of this Office Action given by the Examiner. This Response could not have been presented earlier as the Examiner has only now raised these issues.

The Commissioner is hereby authorized to charge any amount required or credit any overpayment to Deposit Account No. 02-0384 of BAKER BOTTS L.L.P.

Respectfully submitted,  
BAKER BOTTS L.L.P.  
Attorneys for Applicant



Charles S. Fish

Reg. No. 35,870

February 17, 2003

CORRESPONDENCE ADDRESS:

2001 Ross Avenue, Suite 600

Dallas, TX 75201-2980

(214) 953-6507

Customer Number or Bar Code Label:



MARKED UP VERSION OF SPECIFICATION AND CLAIM AMENDMENTS

For the convenience of the Examiner, all claims have been presented below whether or not an amendment has been made. Please amend the specification and claims as follows:

IN THE CLAIMS

1. (Twice Amended) A method for traversing a boundary in a distributed processing environment, comprising:

storing connection protocol information in a connection properties table at a client network for each boundary which may be traversed by the client network;

receiving a request from a client object on the client network for access to a server object on a server network, the server network having a server network boundary;

locating an entry in the connections property table corresponding to the requested server object;

formatting a boundary traversal key from the connection protocol information associated with the located entry in the connection properties table, the boundary traversal key including information to traverse a boundary controlling access to the server network; and

forwarding the request for access and the boundary traversal key to the boundary controlling access to the server network.

2. The method of Claim 1, further comprising determining a connection type from the located entry in the connections property table.

3. The method of Claim 1, further comprising:  
passing the request for access to an object request broker after the client network determines that the request for access is to an object residing outside the client network.

4. The method of Claim 3, wherein the object request broker locates the entry, formats the boundary traversal key, and forwards the request for access and the boundary traversal key to the server network.

5. The method of Claim 1, wherein storing connection protocol information includes storing a boundary identifier, a connection type, authentication information, and connection attributes in the connection properties table.

6. The method of Claim 5, wherein locating an entry includes matching an internet protocol address for the server object to the boundary identifiers stored in the connection properties table.

7. The method of Claim 5, wherein locating an entry includes matching a domain name for the server object to the boundary identifiers stored in the connection properties table.

8. The method of Claim 5, wherein locating an entry includes matching a port address for the server object to the boundary identifiers stored in the connection properties table.

9. The method of Claim 5, wherein formatting the boundary traversal key includes building the boundary traversal key from the authentication information and the connection attributes in a format defined by the connection type.

10. The method of Claim 1, wherein forwarding the request includes forwarding the request for access and the boundary traversal key to the server network boundary.

11. The method of Claim 1, further comprising:  
receiving the request for access and the boundary traversal key at the server network boundary;  
allowing access to the server object if the server network boundary accepts the boundary traversal key; and  
denying access to the server object if the server network boundary rejects the boundary traversal key.



12. (Amended) A distributed computing system, comprising:

a client object on a first network operable to request access to a server object on a second network;

a third network connecting the first network to the second network;

a boundary device controlling access to the second network;

a connections properties table [associated with] in the first network and including an entry for each of one or more second networks accessible by the first network, the connections properties table including connection protocol information for accessing the one or more second networks;

a connection manager operable to generate a boundary traversal key for requests for access to server objects that have a corresponding entry in the connections properties table, the boundary traversal key generated from the corresponding connection protocol information, the boundary traversal key including information to traverse the boundary device controlling access to the second network.

13. The system of Claim 12, further comprising a default connection manager operable to establish a connection between the client object and the server object using a default protocol for requests for access to server objects that do not have a corresponding entry in the connection properties table.

14. The system of Claim 12, wherein the third network is an Internet.

15. The system of Claim 12, further comprising an object request broker operable to facilitate communications between the client object and the server object across the third network.

16. The system of Claim 15, wherein the connection manager is part of the object request broker.

17. The system of Claim 12, wherein the connection properties table includes:

a boundary identifier for identifying the server object on the second network;

a connection type for identifying the type of connection protocol used by the second network;

authentication information for providing identity and credential information to the second network; and

attributes for providing boundary traversal key information to the second network.

18. The system of Claim 12, wherein the connection properties table is stored in a private directory on the first network.

19. The system of Claim 17, wherein the boundary traversal key is generated from the authentication information and the attributes from an entry in the connection properties table corresponding to the server object on the second network.

20. The system of Claim 17, wherein the boundary identifier is an identifier selected from the group consisting of an internet protocol address, an internet protocol address range, a partial internet protocol address, a domain name, a partial domain name, a port address and a port address range.

21. The system of Claim 17, wherein the connection type indicates a TCP/IP connection, an SSL connection, an HTTP Tunneling connection, or a UDP/IP connection.

22. The system of Claim 17, wherein the authentication information includes a user identification and a password.

23. (Amended) A distributed processing system with transparent boundary traversal, comprising:

a client system operable to request access to a plurality of server systems, at least one of the server systems having a boundary device for controlling access to the server system by the client system;

a connection properties table stored in a private directory on the client system, the connection properties table including:

an identification range for identifying the at least one server system having the boundary device;

a boundary type for identifying a type of the boundary device;

authentication information for uniquely identifying the client system to the boundary device and a requested server system; and

attributes for providing traversal information required by the boundary device;

a boundary traversal key generator operable to generate a boundary traversal key for gaining access to the requested server system through the boundary device, the boundary traversal key generated from the connection properties table in response to the boundary traversal key generator locating an entry matching the requested server system.

24. The system of Claim 23, further comprising a network for connecting the client system to the server system.

25. The system of Claim 24, further comprising an object request broker operable to facilitate communications between the client object and the server object across the network.

26. The system of Claim 24, wherein the network is an internet.

27. The system of Claim 25, wherein the boundary traversal key generator is part of the object request broker.